CTIW
CENTER ON TERRORISM
& IRREGULAR WARFARE

Closing the Gaps

A Strategy for Gaining the Initiative in the War on Terror

Naval Postgraduate School, Special Operations Curriculum
Fall 2003
NPS-DA-01-03

Foreword

Several years ago, an inter-service team of officer students at the Naval Postgraduate School studied the problem of cyberterrorism—and co-wrote a white paper that challenged much of the conventional wisdom on the subject. Where the President's Commission and the National Research Council saw the threat as immediate and dire, the NPS team, after a year of study, found that it would be much harder to craft a capacity for sustained cyberterror operations than commonly thought. Indeed, the report argued, from a "standing start," it could take a terrorist group as long as ten years to develop serious cyberspace-based capabilities. And recruiting hackers from the outside would entail security risks that few terrorists would willingly incur. The NPS white paper soon found its way into the Congressional Record, and experts on both sides of the issue acknowledged the thoughtful analysis undertaken by these officers.

Now a new team of officers has done it again—this time by crafting a thoughtful perspective on how to improve our military effectiveness in the terror war. Their intellectual point of departure is the realization that this new war is almost completely irregular in nature, but has caught us at a time when our military is still largely configured for fighting conventional, nation-state oriented enemies. This disjunction between what we have and what confronts us imposes, at least in the early phases of the terror war, a very heavy burden on special operations forces. They are best suited to waging a war against distributed terror networks, but they are the smallest part of the American military. *Closing the Gaps* explains how to get the most out of our special operations forces, and how to begin doing so almost immediately.

The report that follows develops a four-part vision for getting even more out of our special operations forces. The first recommendation advanced is to improve networking within the special operations community. The basic problem is that those who possess actionable information are seldom the ones capable of taking direct action—while those who can take action rely on others for timely, targeted information. Good networking will reduce the amount of friction in the system, and can be achieved at little additional effort and without undue security risks.

While networking within the U.S. military is an important first step, a necessary follow-on is to replicate this kind of connectivity externally. Thus, the second part of the vision articulated in this report consists of systematically exploiting existing military-to-military relationships. This study includes several vignettes, from regions all over the world, where good external networking made a big difference—or could have, if only the rules had allowed. Deeper cultivation of such ties with foreign militaries gives us our best chance of creating the kind of

global "sensory organization" that we must craft if we are to seize and sustain the initiative against networked terror.

The third recommendation advanced in this report grows directly out of the first two. If we are truly to build our own network to fight terror networks, then we must empower our own nodes and cells to act with as much freedom as still allows the senior command to retain "topsight" of the overall conflict. Practically, this means allowing a great deal of operational latitude to forces deployed within various regions. And it means having much trust in the worth of the military-to-military ties developed with our various allies in the war on terror. In a very real sense, this step means following Mao's old dictum to "centralize strategically, but decentralize tactically." Finding the equilibrium between control and decontrol is thus likely to be the central challenge for generalship in this war.

Finally, this report elaborates a fourth aspect of its integrated vision, which keys on recognizing the crucial importance of information operations in this conflict. This war has largely taken on a "hiders and finders" dynamic. At a broader level, our war aims also extend to efforts to try to reduce antipathy among Muslim mass publics. And this is also a war in which skillful information management will enable us to respond swiftly enough to track, capture, or hit fleeting targets when they do pop up. So each aspect of information operations matters greatly. And information strategy should not be limited simply to supporting military strategy. There should instead be an ongoing dialogue between the two, with the considerations of information strategy sometimes influencing the manner in which "kinetic force" is employed.

Taken together, the four components of the vision advanced in this study stand a good chance of improving our war effort. Perhaps the most appealing aspect of the report is that its various policy recommendations are all translatable into actions that can be taken now. These actions require no new force structures; but do call for new ways of organizing our forces and their information flows. And, in the end, what will likely matter most in winning this war is cultivating a new turn of mind—a factor that has always mattered in war, but which is likely to be of over-arching importance to the outcome of this conflict.

Monterey, CA
2003

John Arquilla Fall

Authors

MAJ Jeremy Simmons—Project leader and principal author. Major Simmons' operational experience is in the PACOM theater (1st Group) and participated in OEF-Philippines.

CW2 Chris Manuel—Primary author of Section Three and project leader for USASFC's STAN initiative. CW2 Manuel has extensive experience in EUCOM and CENTCOM AORs (3rd Group) and participated in OEF Afghanistan.

In collaboration with:

CPT (P) Dean Newman	SF, 5th Group, OEF Afghanistan
CPT (P) Steve Basilici	SF, 3rd Group, OEF Afghanistan
CPT Tres Hurst	MI, 3rd Group, OEF Afghanistan
CPT (P) Adrian Donahoe	SF, 1st Group, OEF Philippines
CPT (P) Dwight Reed	SF, 1st Group
CPT (P) Drew Henry	SF, 1st Group
MAJ Marshall Ecklund	SF. 7th Group
MAJ Carlos Perez	SF, 7th Group
LT Brian Harp	USN (SEAL)
LT Bill Denton	USN (SEAL)

Faculty Advisor—Dr. John Arquilla

Table of Contents

Closing the Gaps: Gaining the Initiative in the War on Terror

*"What enables the wise sovereign and the good general to strike and conquer, and achieve things beyond the reach of ordinary men, is **foreknowledge**." -- Sun Tzu, The Art of War*

Introduction

The following is a collective effort by Special Operations / Low Intensity Conflict (SO/LIC) students at the Naval Postgraduate School (NPS) in Monterey, California. We represent a cross section from each service, minus the USMC, who were in operational assignments during the first phases of the Global War On Terror (GWOT). Most of us have served in, or in support of, Operation Enduring Freedom (OEF) in the CENTCOM, PACOM, EUCOM, and SOUTHCOM areas. The purpose of this document is to propose a new way of operating for special operations forces. In a time when small units of action can accomplish incredible feats if given the opportunity, it is time to change from an organization that deploys large joint task forces to one that is capable of self synchronizing at the lowest levels and acting without the presence of large command and control structures. In short, this proposal is about optimizing human resources and creating new economies of force.

We use the term *sensor-shooter* to describe elements that are capable of fulfilling intelligence requirements and are able to take direct action with minimal transition time. We believe special operations forces are best able to meet these sensor-shooter functions. The need for such a capability is self-evident. In the foreseeable future it is likely terror organizations will become increasing dispersed. Secondly, due to the large force commitments to Iraq and Afghanistan, the need for the United States to respond across the globe in short order with small units of action will be required. The net effect of these developments will be to make the War on Terror (WOT) less about large operations and more about small, distributed actions. Since these actions will require the assistance of host nation (HN) forces, the natural fit for these kinds of requirement are the units who traditionally deploy to these areas—SOF.

For this sensor-shooter capability to be integrated into a globally linked network, four critical areas must be addressed. These four areas make up the framework for this proposal. In section one we argue the best mechanism to fuse the global assets with regional assets is a "fused" theater SOC. There is no overriding reason to change command relationships, only the need to be able to task regional assets and fuse them with global assets (human or technical) to quickly respond to threats and, more importantly—to seize fleeting opportunities.

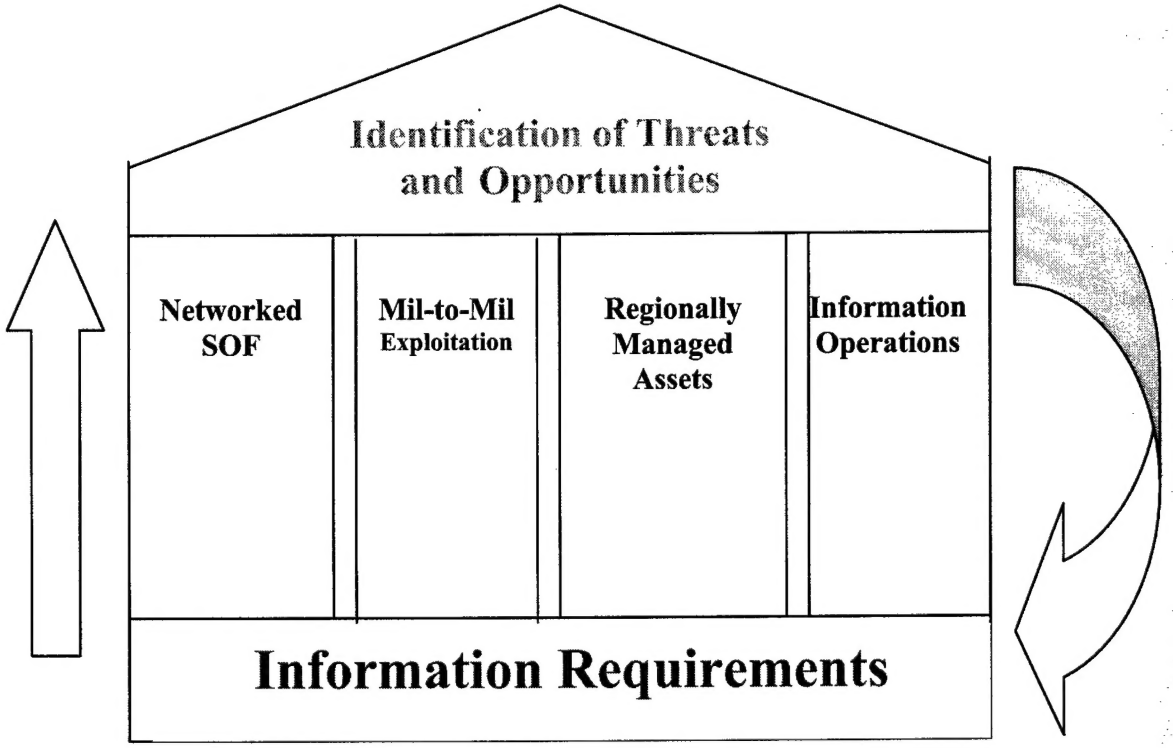
In section two we explain that normal mil-to-mil relationships can be exploited to meet the challenges of the GWOT. Based on our experiences, our current mechanisms do not meet the needs of fighting a truly *global* war on terror.

Section three describes the technical means associated with a regionally managed global network. Many of the systems we describe are in development, but most of these systems

will be available in the very near future. Identifying the CONOP for these new capabilities deserves attention now. This section addresses these issues.

Finally, in section four we discuss the need to integrate information operations into an overall strategy for a theater. These information operations will incorporate cohesive and divisive means.

The end result of our proposal is a realistic, easily established, politically acceptable method for closing the intelligence gaps that exist within our current system. In short, it is a method to allow the United States to be proactive rather than reactive. Having the information to gain the initiative is critical to the task our nation faces in eliminating elements of terror beyond our own borders and preventing attacks on our homeland. We believe SOF can be employed in a manner that will give the nation a decisive advantage over those who wish to do us harm. Hopefully, this document will assist in the development of the required force of the future.



This graphic is a representation of how our four elements of discussion relate to each other. As depicted, information requirements are the foundation of the system. The mechanisms of networked teams and command, mil-to-mil relationships, integration of regional assets into global efforts, and supporting information operations can all be used to gain foreknowledge of emerging threats and alert the chain of command to existing opportunities. Like most such systems, this one is circular in nature. Better use of the four mechanisms listed above will produce better focused information requirements.

Section One- Regionally Managed Assets

Regional focus

We strongly feel the war on terror is a global conflict that, nevertheless, is best managed regionally and prosecuted locally. Consequently, theater commands must have the authority to gather information on regional threats and react accordingly. This is a departure from the *modus operandi* that relies on national assets to react to emerging threats. The problem that exists is one of manpower and mandate. National-level forces have the authority to collect and act, but do not have the manpower to be proactive locally. Regional assets have the manpower but lack the mandate. We suggest the best method to remedy this problem is to fuse national assets with regional operations.

By "fusion" we mean the coupling of regional and national efforts. Not just military assets but intelligence and Department of State efforts as well. Regional SOF should be placed in positions where the United States has a strategic "stake" and used in concert with national level units when applicable. However the relationship between the coupling of regional and national assets emerges, global organizations need a mechanism to "push" information requirements to the regional assets. Likewise, regional units need a mechanism to "pull" information that is pertinent to their efforts on the ground.

We acknowledge a significant amount of effort has been put into making regional organizations more effective[1] and we understand that major organizational roadblocks protect the status quo. Nonetheless, this section will examine how the fusion between global and regional can be accomplished. However, before we examine the methodology, a discussion on the merits of establishing such a system is appropriate.

Counter terror efforts are the domain of the military

The military historian Caleb Carr in his book *The Lessons of Terror* examines the use of terror tactics throughout history and determines that the targeting of civilians to achieve military/political objectives is nothing new in military affairs. He firmly establishes through historical examples that terror has always been a form of war. To treat the perpetrators as criminals is inappropriate, since the act committed was one of war.[2] Therefore, the responsibility falls on the shoulders of those whose mandate involves fighting our nation's wars—the military.

To some, this is an elementary supposition; but it is needed in order to establish that the WOT is a military operation as opposed to series of criminal investigations. Criminal investigations are, by their very nature, reactive. Conversely, a war should be prosecuted in a proactive manner. Military organizations should thus be the proponents for counter-terror initiatives.

---

[1] PACOM has initiated a Joint Inter-Agency Coordination Group/CT (JIACG/CT) and also improved networking capabilities.

[2] Caleb Carr, *The Lessons of Terror* (New York: Random House, 2002), 240-247.

Organizational structure and authority for information collection

Any modification to existing organizational structures must first begin with some simple questions. Why change? What is not working?

The combatant commanders (CCs) have regional responsibility and autonomy to do what they feel is necessary to advance the policies and defend the interests of the United States. The CC is granted the authority to "conduct special operations activity or missions unless otherwise directed."[3] However, this authority does not grant the CC intelligence gathering responsibility. Title 10 Section 167 USC states, "This section does not constitute authority to conduct any activity which, if carried out as an intelligence activity by the Department of Defense, would require a notice to the Select Committee on Intelligence of the Senate and the Permanent Select Committee on Intelligence of the Senate an the Permanent Select Committee on Intelligence of the House of Representatives." Therefore, the authority required to gather HUMINT on a grand scale lies with assets and organizations that the CC does not control. In short, the CC has the mission but not the authority.

Conversely, national level assets and organizations (CIA, DIA, Special Mission Units or SMUs) do have the authority (Title 50 USC Chapter 15) to conduct intelligence-gathering duties. The problem with above-mentioned units is that they do not have the number of personnel to spread out across the globe with any hope of thoroughness or of protracted involvement. Inevitably, these assets will be forced into reactive position because they do not have the ability to "see" opportunities that can spark proactive measures. So, just as the theater CC has the men but not the mission, the organizations with the mission do not have the assets that allow the US to be as effective as we can be. This kind of structural constraint defaults the initiative to the enemy.

Each theater is unique. The environmental factors that define the CENTCOM area of responsibility (AOR) are not the same in PACOM, SOUTHCOM, etc. PACOM in particular represents a region that is defined by legitimate governments but which is plagued with local guerrilla/terrorist organizations. The links between middle eastern terror groups/states, the drug trade, fund raising, and terror training camps are clear, yet it has been the stated preference of regional governments to try to counter these threats themselves. Since these governments have proven only marginally effective in doing so, cooperation is the path to take in PACOM. Cooperation is infinitely more complex than unilateralism and requires prolonged commitment. It is counterproductive to try to force unilateral efforts onto a nation/region with those the host nation does not know. We acknowledge there are exceptions, but by and large, such reactionary efforts create distrust with regional allies. Cooperation, on the other hand, breeds trust.

Regionally based special forces units are the ideal force to build trust. SF teams are consistently deployed to countries in which a threat to the United States exists. But, these units are rarely tasked with intelligence requirements when deployed. The line between Title 10 and Title 50 authorities is further apart than it needs to be. If Title 10 authorities would be interpreted more liberally, the ability for USSF to conduct relatively benign

[3] Title 10 USC Section 167, Chapter 6, Part I

information collection could be maximized. We are not advancing the notion that USSF should have Title 50 authority in its entirety, but rather that Title 10 authority be expanded. This requires a formal legal review but as we interpret the USC, the expansion of Title 10 authority can be accomplished under the justification of national security concerns. Recommendations: (1) Expand Title 10 information gathering authorities; and (2) Integrate USSF into actions that fall under the designated units with Title 50 authority.

One solution is to empower the regional commander with the authority to task lower-tiered special forces units who are conducting mil-to-mil missions to gather information while deployed. We believe the regional special operations command (SOC) should manage this responsibility. The SOC should be "fused" with national level assets (all the agencies plus, when applicable, SMUs) so that a coordinated effort is produced and the ability to "pull" information from national databases is possible. The national level organizations would also have the ability to "push" requirements to the regional SOC. The result of this effort would be a theater "collection plan" with a global input mechanism.

Creating and maintaining a collection plan

In Robert Leonhard's re-examination of the principles of war for the information age he advances the idea that the organization with the information should make the decisions.[4] Leonhard adds, "Part of the reason we have yet to see a clear exploitation of information technology is that we are clinging to outdated doctrine that calls for decentralized command in control."[5] In other words, to optimize human and technological assets the regional command must have the authority to act. Only a regionally based organization that is fused can appropriately task units of maneuver to gather information/intelligence. To place this burden on the global command will overwhelm that system and cause it to be slow in its response. Therefore, reform should be focused not on decentralization below the regional command, or worst yet, consolidation of authority at the national level, i.e. SOCOM. Authority is rightly placed in the hands of the regional commander. This will eliminate duplication with the national command while maximizing regional assets. The end result will allow the tasking agency—the SOC—to spread out the collection tasks over a variety of collection platforms, technical, OGA, DoD national assets, and SOF (white SOF). This will produce a better intelligence picture of the battlefield. At a minimum, the country team should direct USSF to "develop" the picture of the area in which the team is deployed. But, if the country team has "tasking" authority, it must be plugged into the regional strategy, and must be integrated into global strategic calculations.

What do we mean by collection plans?

Collection plans are not just enemy-based; they also focus on terrain, demographics, and friendly troops. A grand collection plan will allow a SOC (and/or country team) to task

[4] Robert Leonhard *The Principles of War for the Information Age* (Novato, CA: Presidio Press, 2000) 200-202
[5] Ibid. 201

SOF units to answer questions. These questions are not big ones like, "Is AQ operating in this country?" Rather, they are smaller, more focused information requirements that point to larger questions. For example, an ODA may have the opportunity to conduct training with a unit whose leadership is suspected of being involved in nefarious activities. That ODA may be able to provide details that will allow a regionally fused CT cell to piece together other bits information to get a better picture of the involvement between government forces and criminal elements. Collection plans must focus on understanding the "battlefield" (both friend and foe) and then preparing the area for action. In a mathematical sense, a strategy based on a grand collection plan would look like this: IPB + OPB = Initiative. Initiative = Preemptive and preventive actions.

What questions need answering?

Insurgents and terrorists operate asymmetrically because they have little choice. If they could win their battles through symmetrical means, then they would employ conventional tactics. Steven Metz provides a conceptual framework for understanding the nature of the threat.[6] Among his useful insights is the idea of asymmetry at the strategic level. Asymmetrical approaches permit insurgents to fight with their strengths while negating their weaknesses. Collection plans must identify the strengths and weaknesses of both the enemy and ourselves. A grand collection plan will prepare the battlefield by identifying strengths, weaknesses and vulnerabilities of the enemy and the HN. Also, it should address the physical as well as the human environment. USSF does this on a regular basis but the data is stored in the team rooms where it serves no strategic utility. *Recommendation*: A databasing system that is better than the already existing SODARS should be developed in order for teams (as well as decision makers) to access information easily. Contracting a firm to develop a secure, easily networked, system should be done without delay.

What to do with the information?

Operations can be developed through a combined collection plan. They may not necessarily target AQ elements, but certainly that is one goal. In the very near future, deployed teams will have the ability to gather digital data on individuals, installations, known criminal threats (e.g. the local kingpin), and other bits of information that are only limited by the imagination.

Imagine a time when preparing to deploy to a particular location can be accomplished without having to "prep" the area. This will reduce response time tremendously and completely surprise any threat in the area. Data based on collection plan input is the key to accomplishing this. Similarly, since a vibrant database will exist, a strategy can be developed to reinforce existing rapport established by SOF personnel. If a particular HN unit is known to be effective and competent, they should receive more attention from US advisors, not less. The principle of economy of force applies here. Trying to spread the advisory wealth is much less effective to the larger effort than relying on a small number of units who are extremely competent. Robert Kaplan notes that this has been the method

[6] Steven Metz, "Strategic Asymmetry," *Military Review*, July-August 2001[journal online]; available from http://www-cgsc.army.mil/milrev/english/JulAug01/met.asp; Internet; accessed 1 October 2003.

of choice for many imperial empires in his *Atlantic*[7] article. In other words, the goal is to develop relationships with a few units that can be used in a time of need. Databasing information will not only help identify which units will be useful but also which USSF units have personal contacts within the targeted unit. The alternative is to assign permanent advisors. Since our current personnel structure does not facilitate these kinds of "permanent" deployments the best solution to accomplish the same goal is through databasing contacts.

Additional dimensions to collection plans

As noted, the collection plan cannot be limited to just the enemy and HN forces. It must include demographics, and alliances. For example, knowing what factions are players in the region is important. Can we use them as surrogate forces against local threats? Can we use IO campaigns to get the two factions warring against each other? Can we foster suspicion between them? What are the "fault lines"? What are possible PSYOP and deception themes that could work in a particular area?

Collection plans must also target the population. Populations are key centers of gravity in asymmetrical warfare; ground truth about those populations can assist future operations significantly. A good example of population-based "targeting" occurred during Operation Enduring Freedom- Philippines when the population of Basilan Island was surveyed on a variety of subjects. It turned out that lack of potable water was placing a terrible burden on the residents. Consequently, the US was able to meet many of its objectives by simply digging wells. This went a long way toward connecting the government to the people and alienating the terrorist from the same villagers they depended on so heavily for support. The point being that IPB in asymmetrical warfare is far more than just focusing on friendly and enemy situations.

This kind of information can be collected by USSF by simply tasking them to find out the leading complaint of the local population. But, they must be tasked. Having a standing set of questions that each team should answer is not the answer. This kind of solution will inevitably generate a lot extraneous information. For a collection plan to be effective, a clear task should be associated with a specific collector.

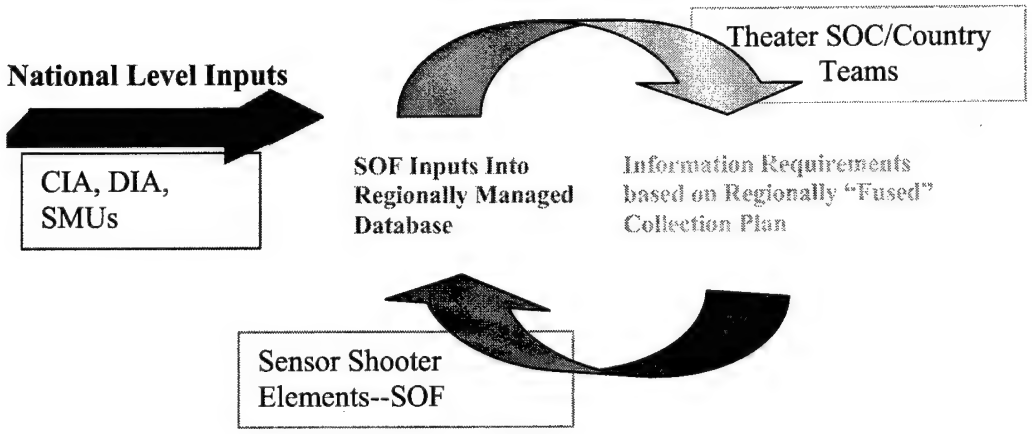
Conclusions

We feel a true regional focus has not yet been developed in the war on terror. Although there are numerous successes, SOF—particularly USSF—have yet to see their information collection abilities optimized outside of large-scale contingency operations. Properly trained members of SOF have solid tradecraft required to conduct the type of HUMINT activities required. Granted, there are varying degrees of skills, but much of the HUMINT type work can easily be done with the current skill set possessed by white SOF units. However, before these talents are realized two things must occur. First, USSF need to be tasked. The theater SOC and the country team need to recognize there is valuable information to be gleaned from SOF deployments. Once this is acknowledged,

[7] Robert Kaplan. "Supremacy by Stealth," *The Atlantic*, July 2003. [journal online]; available from http://www.theatlantic.com/issues/2003/07/kaplan.htm; Internet; accessed 1 October, 2003

deployed teams will be able to understand the kinds of questions that need answering. Of course, this idea is predicated on the assumption that USSF will be deployed in countries where a threat exists. Second, a user-friendly system needs to be developed that will allow for effective databasing.

These two recommendations are integrally linked. Once an effective databasing system is available that is focused through a regional collection plan, a bottom-up strategy will emerge. Tasks will be assigned by the regional SOC, the information will be placed into the system, and this information will lead to better focused taskings.



Section Two-Mil to Mil Engagement
Exploiting Situations, Locations, and Information

The primary non-operational deployment for SOF is the JCET. JCETs support unilateral training objectives and serve as a means for a combatant commander to further his cooperation objectives in theater. The theater cooperation strategy for SOF units is really nothing more than a prioritized list of countries that are chosen for a variety of reasons to receive training from the US military. There are numerous other missions that the CCs use for mil-to-mil engagement, however, the staple seems to be the joint combined exercise training program.

However, theater engagements under Title 10 restrictions have no real impact on the WOT. Little attention by JCET planners is focused on conducting counter terrorist operations during these "engagements" and even less of developing intelligence. Therefore, we feel the JCET program is a peacetime program that has outlived its usefulness. As discussed in the previous section, Title 10 authorities restrict the ability of the CC to optimize the potential of his regional personnel for battlefield development.

Recommendation: Shift SOF personnel away from fulfilling JCET commitments to counties where an active threat does not exist. Turn these missions over to conventional forces or the USMC, or simply reduce our existing commitments. However, USSF should maintain contact with HN Counter Terror (CT) units when possible. USSF should more to spend a preponderance of their time working in threat countries.

To demonstrate the effectiveness of having USSF deploy to countries where a threat exists, we will examine four vignettes where deployed teams were in a position to exploit situations but did not due to existing ROE. If given more robust authorities, these ODAs could have exploited the following situations and given the CC a much clearer picture his AOR. In one case, Nigeria, terrorists could have been eliminated.

Republic of the Philippines, summer/fall 2001 – potential to exploit situations

In the spring of 2001 the Abu Sayyaf Group (ASG) seized twenty hostages from the Philippine Island of Palawan and returned with them to their home base on Basilan in the southern Philippines. Three of the hostages were Americans, Guillermo Sobero, and the missionary couple Martin and Gracia Burnham. In February of 2002, the PACOM commander decided to send a contingent of US Special Forces personnel to the southern Philippines to assist the Armed Forces of the Philippines in combating the ASG. This operation was called Operation Enduring Freedom Philippines. It took close to six months from the time planning started to the time operations began.

At the time of the hostage takings, USSF team members were finishing up the training of a level-two counter terrorist force of the Philippines Armed Forces (AFP) on the main island of Luzon. Due to the intimacy of the training, a bi-lateral capability started to develop between the Philippine CT Force (Named the Light Reaction Company or LRC) and the US force. An opportunity arose for US personnel to accompany the LRC upon the completion of the training to Basilan to conduct operations to recover the hostages. But this was not seriously pursued by the United States. Had the USSF personnel

accompanied their newly trained experts, a great deal of information could have been gained from their presence on the ground on the competency of the Armed Forces of the Philippines (AFP) and the ASG terrorist group.

The first JCET executed after the 9/11 attacks in the PACOM AOR was back in the Philippines and working again with the LRC. The LRC had been on six months of continuous operations since their graduation. The hostages had yet to be recovered and one American had been killed. The JCET was conducted on Luzon, but in the midst of the training another guerrilla/terrorist incident occurred in the Southern Philippines causing the LRC to leave training for operational use. The offer was again extended to have Americans (just a few) accompany the LRC on the mission as observers. Again, this offer was not seriously considered by the US chain of command. The details of why this option was not pursued were not revealed to the ODA, nor are the decisions germane to our point. The point is, USSF is often presented with opportunities to develop the intelligence picture of a particular situation.

The United States, especially those of us who operate in the Philippines, has known of the insurgencies of Luzon (New People's Army or NPA), and the Southern Philippines (MNLF, MILF, ASG) for years. Every 1st Special Forces Group team that has conducted a genuine Battle Focused Analysis (BFA) on the Philippines has correctly identified the threat to the interests of the United States these groups pose.

The linkage between Middle Eastern rogue states (Libya) and the Philippine separatist movements were well known before 9/11 occurred[8]. On-the-ground reconnaissance of the southern Philippines in anticipation of having to deal with these threats could have occurred both before, and immediately after 9/11 with teams that were already in country and had established contacts, specifically with the LRC. This is the salient point of the case study. More could be done with teams that are already in position, but regional commands must have the authority and the incentive to do so. This vignette is an example of a situation that could have been exploited to advance the regional commander's picture of the battlefield.

Mali; Africa, summer 2001 – potential to exploit location

A Special Forces battalion was conducting a JCET in Mali in June 2001. The Chief of Station and EUCOM knew terror organizations in northern Mali where trafficking weapons for terrorist operating out of Algeria. A tremendous opportunity existed here. The Special Forces soldiers training with the Malian Para-regiment could have prepared for 3-4 weeks and then conducted a follow-on mission to destroy this logistical node. As it turned out, in the post September 11 atmosphere, EUCOM tried to recreate this opportunity but for reasons unclear to the operators, was unable to do so. This is another example of how opportunities, when presented, should be exploited.

Even if the permission to conduct direct action had not been granted, the location alone should have prompted someone to task the Special Forces teams to gather information

[8] Open source data. Marites Danguilan Vitug & Glenda M. Gloria. *Under the Crescent Moon: Rebellion in Mindanao* (Quezon City, Philipinnes: Institute for Popular Democracy, 2000)

and plug it into a regional database. If the decision makers and their staff had been thinking proactively, specific lines of communication (LOCs), staging areas, local trustees, could have been identified for exploitation. To be frank, regional SOCs and, more importantly their staffs, sometimes just don't think that way.

Abuja; Nigeria, fall 2001 – potential to exploit information

The same Special Forces battalion as described above was conducting another JCET in Nigeria. The station chief had information that a ship containing arms possibly for AQ was going to dock in Lagos, Nigeria. Nigeria is a crossroads for many terrorist organizations, due to the porous nature of its borders. Additionally, Nigeria is so immersed in inter-religious strife that many terrorist cells are established. In this instance, the CIA Station Chief was very pro-active and wanted to use the in-country SF teams to interdict this shipment of arms. For reasons unbeknownst to the team, SOCEUR and EUCOM said no.

This is another example of how information exploitation could have occurred but did not. We acknowledge that there may have been overriding political concerns that precluded the use of SF, but this same sequence of events seem to happen all the time. This indicates that a systemic problem exists.

The SF teams' capabilities could have been utilized if just everyone in the decision cycle had been informed of the possibilities. SOCEUR, with a fused CT cell, could have looked at that JCET as an opportunity to conduct IPB, OPB, and AFO. The agency representative could have pulled information from the station chief and then shared that with the regional SOC prior to deployment. All of this would have prepared the team and the appropriate decision makers for the potential for action. A common perception of our community is that many of our senior leadership are risk adverse. Although there may be cases where this is completely true, we believe that risk adverseness is more a function of incomplete information than it is a personality trait. We believe that a regionally managed fusion cell that tasks deployed ODAs could streamline information and give decision makers the necessary information prior to putting American lives at risk.

Uzbekistan, fall 2001-a success story

An ODA was in Chirchik, Uzbekistan in August of 2001. It had been working with the Peacekeeping battalion of the Uzbeki army since Dec of 2000 on a series of Combined Threat Reduction (CTR) missions designed to enhance the CH 7 peacekeeping ability of the Ministry of Defense. As part of the Program of Instruction, the ODA had coordinated to use a training area southeast of Chirchik for small-unit tactics as it had on previous deployments.

Just prior to departing for the training area, representatives from the Ministry of Defense approached the ODA commander and informed him that he needed the ODA to relocate its training. At the time, the THREATCON was Charlie, and August was typically the most active time for the Islamic Militia of Uzbekistan (IMU) to attack Tashkent, just west of Chirchik. The ODA was aware of the likelihood of such a possibly, and was prepared to work in all threat environments. The ODA commander pressed the Ministry of

Defense for more information, asking for reasons why he should relocate his training. The ODA had already been witnessing Uzbeki air interdiction "training" missions that Uzbeki soldiers had quietly confided weren't really training. The ODA had reported live helicopter and fixed wing interdiction missions. Live ammunition is not wasted on training in Uzbekistan.

When reporting all the information to the DAO, the DATT informed the ODA that they had no information of IMU activity or COIN efforts by the Uzbeki government. Had the ODA not been in place, they might not have learned that IMU or Uzbeki units were engaged so near Tashkent, the capitol.

The ODA complied with the Ministry of Defense's request to change location. The ODA chose a new training ground that it had not yet had an opportunity to investigate as part of its area assessment. Consequently, the ODA spent weeks maneuvering in rural areas of Uzbekistan between Chirchik and Tashkent, and south of the Kazakh border. Adjacent to the training area was an enormous signal intelligence station. The ODA deliberately acquired numerous photos of this station without authorization. Nonetheless, the intelligence community found these photos to be very valuable upon debrief.

The ODA's peacetime mission placed it in a position where it provided access to critical information for real world intelligence, and this happens often. The ODA was able to exploit information without any direction from a centrally organized intelligence apparatus. This information could have very easily been overlooked since it was by no means within the ODA's "lane" to report such items. In this case, the system worked, but only because the DAO and SOCCENT were curious about what the ODA saw. In our collective experience, most of the time country teams have little interest in ODA activities.

Potential exists but must be tapped

The lesson to be learned from these vignettes is that if USSF are deployed to threat environments they are positioned to exploit situations, locations, and information. Only white SF are capable of doing this. National assets by their very nature are reactive. However, the emerging threats we are aware of are only half the story. Imagine how our knowledge could be increased if we actively exploited the situations that developed *around* a deployed ODA. The implication of tapping such a resource is that a global sensory network would emerge that had the ability to respond. White SOF elements are the perfect sensor-shooters. But, this capability will remain on the sideline if it is not **tasked** to gather information. Listed below are some additional benefits of optimizing deployed USSF teams.

Merging Regional and National assets

Think of the potential for action if white and black units would "merge" on a regular basis. This kind of organization reform would maximize the access gained by regional assets with authority to gather granted the national personnel. These units could carry out the benign function of training HN personnel while still being capable of gathering

intelligence. These units of action can be the 'on-the-ground' element that will facilitate operations between the US and its counterparts in the indigenous military or paramilitary forces of the target country, while at the same time filling intelligence gaps. In truth, the possible scenarios where a "merged" unit of action could be utilized are only limited by the imagination. But, one thing is certain. By merging these units the *global* knowledge is integrated into the *local.* This is critical for an effective global network to emerge.

CP of WMD

Radiological mapping includes methodical probes of potential target areas to gain radiological background data. Mil-to-mil missions can act as a cover for baseline mapping of potential trouble spots, like ports. Even if these activities were conducted openly with assistance from the HN, the fear that the US can detect small amount of radiological material can have a tremendous collateral effect of those who may attempt to traffic such material. In a sense the actually capability is less important the message sent to potential traffickers. This area is ripe for an information strategy that is managed by a regional organization. This brings up another point. Traditional CP of WMD operations are primarily unilateral. One of the authors (who was on a CP of WMD ODA) feels the best method conduct CP of WMD operations is through the use of surrogates. The HN has the personnel and will often act as filter to potential terrorists. Again, the perception of a capability can often achieve the desired effect, which is to deter trafficking of dangerous materials. Obviously, there must be a merging of efforts between regional and national assets, but it is possible.

Conclusions

This section discusses the potential of deployed SOF personnel. Special Forces Companies and Detachments, and to a lesser extent, Navy SEALS, are often deployed in areas where information gaps exist. By exploiting the opportunities these units often find presented to them, a great deal of operational data can be gained to help the CC develop a more accurate picture of his AOR. However, for deployed units to fully maximize their potential, they must be tasked with specific information requirements while they are deployed. The reason to give more authority to regional SOF is simple. It allows the United States to be proactive in its counterterror efforts instead of reacting to a crisis or old information. It will increase response time. USSF has the skills, and the local knowledge to perform both sensor and shooter functions. "Merging" national and regional assets can further enhance this capability. This sensor-shooter network of regional assets will become even more powerful as new technologies emerge that allow units to be linked to distant command-and-control mechanisms as will be discussed in the next section.

Section Three - Networked SOF

This section of our proposal explains how "network-centric" warfare can maximize the effectiveness of SOF. Much of what is contained in this section is doable now. However, the real potential resides within the advanced technologies currently in development. The potential and power of deployed SOF with these emerging technological capabilities has tremendous doctrinal implications. Decision makers need to start thinking about how to exploit these empowered units. What we have suggested in the previous two sections is a start but does not fully capture the true potential of widely dispersed personnel. Two key ideas should be in the mind of the reader as he or she examines the following section. First, dispersed units will have the ability to receive information from command and control elements and conduct the necessary planning and preparation without the presence of deployed C4I. The same functions of traditional organizational structure will still exist but they can be conducted virtually. Second, the networking capability of deployed teams will allow them to "self synchronize" laterally with support units. This will greatly reduce the necessary signature prior to any action and lend itself to creating initiative on the part of US counterterror efforts.

What is networked SOF?

To begin this discussion we will review the concepts advanced by Vice Admiral (ret.) Arthur K. Cebrowski and John J. Garstka.[9] Cebrowski advances the idea that with emerging technologies—specifically, Internet protocols—information can be easily created, distributed, and exploited. The information is contained within a network and thus, the power of the network is proportional to the square of the number of nodes in the network. This is called "Metcalfe's Law"[10]. The result of this power on command and control is twofold: one, the information network increases the "speed of command", and two, the network allows units to self synchronize from the bottom up.

Cebrowski and Garstka add that speed of command has three parts: "(1) The force achieves information superiority, (2) Forces act with speed, precision, and achieve the massing of effects versus the massing of forces, and (3) The rapid foreclosure on enemy courses of action." This will, in theory, disrupt the enemy's strategy and preempt an action from taking place.

Cebrowski, being a naval strategist, explains these concepts through examples of moving battleships into position to "preempt" offensive action of a hostile force. Much of the Navy's efforts at the Naval Postgraduate School are focused into making his operational concepts a reality. Likewise, SOF is researching how to network units of maneuver like ODAs and their surrogates with UAVs, Strike Aircraft, etc. These are all useful and necessary but are generally aimed at conventional, mid to high intensity conflicts. However, we propose that these same operational principals can be applied to an entire region and done so on a continual basis. In other words, SOF teams deployed throughout

---

[9] Arthur Cebrowski & John Garstka, "Network Centric Warfare: Its Origin and Future," *Naval Institute Proceedings,* January 1998 [journal online]; available from http://www.usni.org/Proceedings/Articles98/PROcebrowski.htm; accessed 29 March 2003

[10] George Gilder. "Metcalfe's Law and Legacy" (*Forbes ASAP*, 13 September 1993) as cited in the above mentioned *Proceedings* article